JCA-NETセミナー
サイバースパイとは――加害者にも被害者にもならないために

としまる
toshi@jca.apc.org
2025/11/19

サイバースパイとは――加害者にも被害者にもならないために

高市政権が「スパイ防止法」に前のめりになり、危惧の声が拡がっています。また、安保・防衛三文書についても早々と見直しの声も上がっています。臨時国会の議論を経て、次期通常国会では、具体的な法案や組織体制などが政府から提示されることも確実視されています。

　インターネットやサイバー領域でのスパイ活動には、伝統的なスパイ活動にはない様々な特徴があります。いわゆる「敵」とみなされた国のネットワークに侵入して情報を収集する活動と自国内部の反政府活動や外国籍の人たちの情報 収集など様々なケースが明確に区別されないまま行なわれる可能性があります。

　今回、政権が構想しているスパイ活動は、諸外国の諜報機関による活動を念頭に置き、日本にこれまでなかった機関の創設となると思われます。公開情報の収集から違法なハッキングによる情報収集まで、違法・合法、国内・国外の枠を越えた活動が展開されることが予想されます。更に、スパイの域を越えたサイバー攻撃や実空間での軍事的な攻撃に必要なプロセスとも重なる場合も想定されます。いずれもサイバー領域では官民連携が必須であり、更に、サイバー領域での活動とソーシャルエンジニアリングと呼ばれる従来型の人間関係を介した情報収集とも連携がとられることになるでしょう。

次の順番で話します

1．**ターゲットを絞ったサイバースパイ**
「高度持続的脅威」という具体的なサイバースパイ・サイバー攻撃のケースに沿って説明します。
2．その上で、**サイバースパイ・サイバー攻撃全体像**をごく簡単に紹介します。
3．高市政権が狙う**スパイ機関創設の経緯**、特に**維新との合意文書**に明記された事柄の問題点を指摘します。
4．私たちの**対抗手段**について、いくつか提案します。

ターゲットを絞ったサイバースパイ

高度持続的脅威（APT） 架空の物語

「想像してほしい。勤めている会社がハッキングされたとしよう。朝、オフィスに入ってパソコンを起動すると、ポップアップメッセージが表示される。ITスタッフがシステムを再インストールし、パスワードをリセットしたという。新しい認証情報をIT部門で受け取りに廊下を歩いていると、噂話を耳にする。ここ数ヶ月間、ネットワークは完全に侵害された状態だった。攻撃者は数十のシステムにアクセスし、ファイルサーバーやデータベースを嗅ぎまわって回っていた。最終的に、彼らは慎重に選んだ機密文書を数百メガバイト分盗み出すことに成功した。技術に興味がある人間なら、まず最初に疑問に思うのは、攻撃者がどうやってネットワークに侵入したのか、そして彼らを追い出すには何が必要だったのかだろう。だがおそらく、すぐに次の疑問が浮かぶだろう。攻撃者は誰なのか、どんな情報を探していたのか、盗んだデータをどう悪用するのか。おそらくあなたがこうしたことを考えるのは、法的措置や復讐を望んでいるからではない。むしろ、そうした答えが全体の状況を理解する助けになるからだ。事件の背後に誰がいて、どんな動機があったのかが分からなければ、ネットワークが修復されたという事実だけでは人間の好奇心は満たされない。」

出典：Timo Steffens, Attribution of Advanced Persistent Threats——How to Identify the Actors Behind Cyber-Espionage, Springer 2020

ターゲットを絞ったサイバースパイ

古典的な方法(クリフォード・ストール『カッコウはコンピュータに卵を産む』(草思社文庫)

　犯人らは大学のコンピュータを中継サーバーとして利用し、実際の標的システムに侵入していた。数ヶ月にわたり、ストールは接続データを分析して次々と現れる中継サーバーを特定し、これらの侵害されたコンピューターの無自覚な所有者に連絡を取り、さらなる接続詳細を聞き出して次のジャンプサーバーへと導いた。最終的に警察や情報機関と協力し、KGBに雇われたドイツ人ハッカーをハノーバーで突き止めることに成功した。
(https://ci.nii.ac.jp/ncid/BB25836355)
⇒現在では、足跡を隠す様々な技術があるので、このような追跡手法では攻撃者を特定できない。

ターゲットを絞ったサイバースパイ
高度持続的脅威（APT）とは

APTは標的型攻撃攻撃の一種。

定義

- 高度持続的脅威（Advanced Persistent Threat：APT）とは「特定の組織や個人を標的として長期にわたって行われるサイバー攻撃」「攻撃者は複数の手口を組み合わせて巧妙に侵入し、検知されにくい形で情報の窃取やシステムの破壊などを狙」う。(KDDI https://biz.kddi.com/content/column/smb/advanced-persistent-threat-tact/)
- 純粋な金銭的動機ではなく、戦略的・政治的に利用可能なデータの取得を目指すグループを指す。このグループは政府またはその代理として活動する。(Timo Steffens, Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage Springer 2020)
- 特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃(情報セキュリティ白書2025 https://www.ipa.go.jp/publish/wp-security/j5u9nn0000004wk0-att/ISWP2025_ALL.pdf

高度とは ネットワークへの不正な侵入を早期に発見できないような手法をとる
持続的とは 攻撃者が意図的に標的を選び、長期間・繰り返し攻撃を試みる。
脅威とは 攻撃の背後にいる主体を示す用語。戦略的動機を持つ主体を指す。

ターゲットを絞ったサイバースパイ

高度持続的脅威（APT）とは

「APT攻撃は「高度かつ継続的な脅威」という意味のとおり、長期間にわたりサイバー攻撃を継続し、機密情報を盗み出したり、重要なシステムを破壊することを目的としています。このため、従来のセキュリティ対策を巧妙にすり抜け、少しずつ組織内部へ侵入していきます。標的型攻撃の中でも特に発見が難しく、攻撃が発覚した時にはすでに甚大な被害が生じている可能性があります。」(KDDI https://biz.kddi.com/content/column/smb/advanced-persistent-threat-tact/)

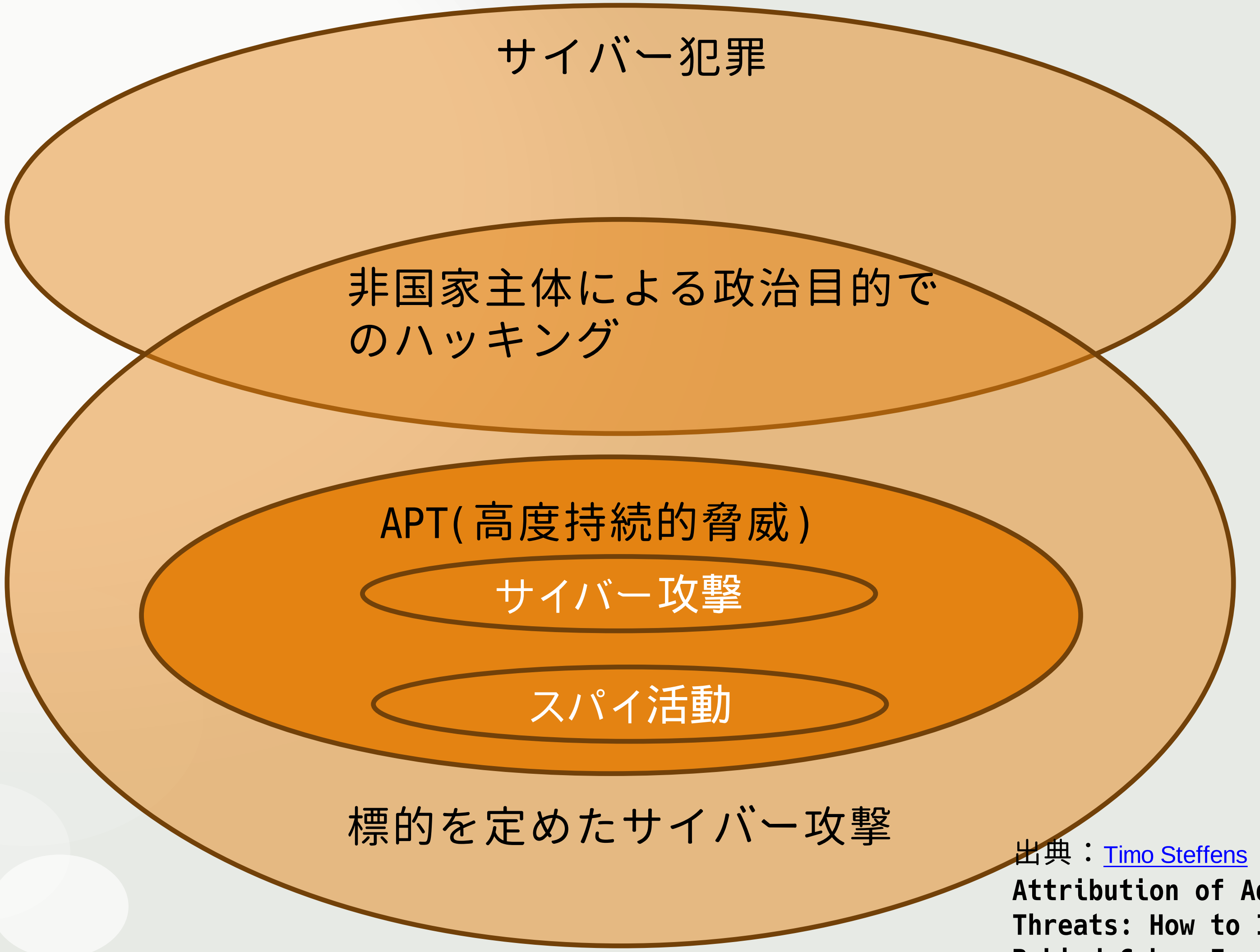
標的組織のネットワークに侵入する手口として、VPN機器や Web サーバー等のネットワーク境界に接する機器に対し、脆弱性や設定不備を悪用して侵入したり、何らかの方法で得た認証情報（ID とパスワード等）を使ったりして不正アクセスし、組織内のネットワークに侵入する手口がある。IPA では、このような手口による攻撃を「ネットワーク貫通型攻撃」と呼び、2023 年以降、この手口による攻撃に関する注意喚起を行っている[※93]。

また、中国の国家支援型攻撃グループとされる「Volt Typhoon[※96]」のように、ネットワーク境界に接する機器の脆弱性を悪用して標的組織内のネットワークに侵入後、将来的な重要インフラシステムへの攻撃のため、Living Off The Land（LOTL）戦術[※97]を用いて長期間にわたり当該ネットワークへのアクセスを維持する攻撃者も存在するため、このような手口にも注意が必要である[※98]。なお、LOTL 戦術は、ネットワーク貫通型攻撃

IPA(情報処理推進機構)情報セキュリティ白書2025p.24

ターゲットを絞ったサイバースパイ

高度持続的脅威（APT）とは



出典：[Timo Steffens](#)
Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage Springer 2020

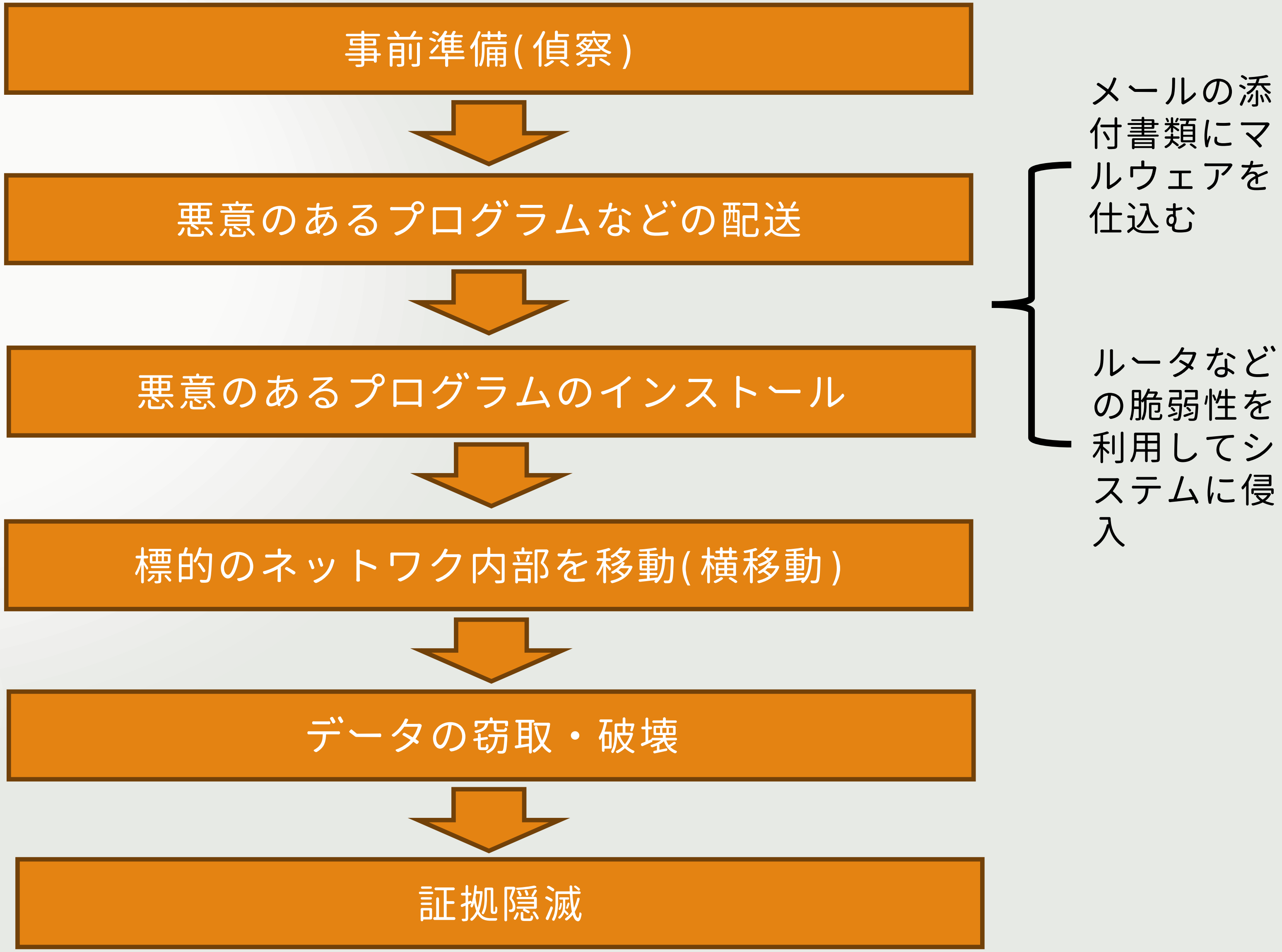
ターゲットを絞ったサイバースパイ

高度持続的脅威（APT）とは

典型的なAPTによる攻撃

- **事前準備** 攻撃者は無作為なシステムを標的とせず、政府が求める情報をもつ可能性のある組織のネットワークを選定する。
  - 実際の攻撃よりずっと前に行われることが多い。
  - 情報はソーシャルメディアやニュースサイト、その他の外部ウェブソースから収集される可能性がある。
- **配送** 悪意のプログラムをメールやウエッブ経由相手の組織構成員に送付する
- **(横)移動** ネットワーク内部でアクセス・認証情報などを収集しながら標的のネエトワークを移動

(参考)IBM「横移動とは」https://www.ibm.com/jp-ja/think/topics/lateral-movement

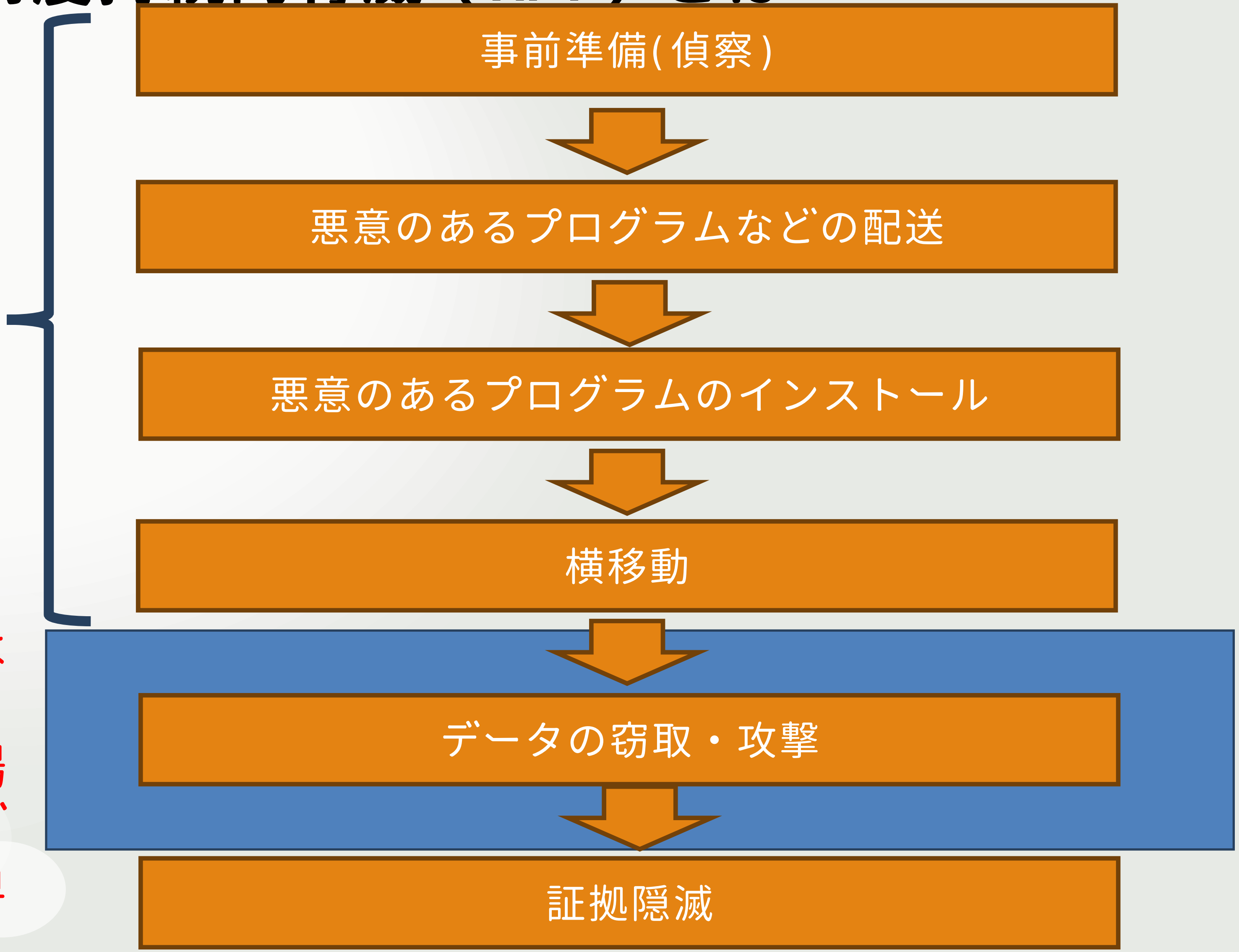


ターゲットを絞ったサイバースパイ

高度持続的脅威（APT）とは

- この部分は、スパイ活動の場合も攻撃の場合もほぼ共通する
- 注目されている「先制的」とか「能動的」といった概念は、一般的にはこうした活動が明確に理解されていない。

実際に攻撃が表面化するのはこの時点でのこと。「攻撃」が事後的であった場合でも、実際の偵察行動など一連の行動はときには数年単位で事前に行なわれる。



APTの事例

中露朝の関与・支援が疑われる主要なサイバー脅威主体

	主体の識別名（別名の例）	関連が疑われる国家機関等	関与したサイバー攻撃事案、標的等
中国	APT1	中国人民解放軍	・原子力メーカー等米国6組織からの情報窃取（2006～2014年）
	APT10	中国国家安全部	・米国の企業・政府機関からの技術情報の窃取（2006～2018年頃） ・世界中のIT管理事業者（MSP）への侵入（2006～2018年頃）
	APT31		・英国国会議員のメールアカウントへの侵入（2021年）、同国選挙管理委員会への侵入（2021～2022年）
	APT40		・米国等の企業、政府機関等からの技術情報の窃取（2011～2018年） ・台湾政府機関への侵入（2018年） ・豪州国内組織からユーザー名、パスワード等を窃取（2022年）
	APT41		・米国等世界中の100社以上への侵入に関与（2014～2020年）
ロシア	APT28（Fancy Bear）	ロシア連邦軍参謀本部情報総局	・各国政府機関等を標的とした大規模なブルートフォース攻撃（2021年）
	APT29（Cozy Bear）	ロシア対外諜報庁	・米国の政党への侵入（2015年） ・ワクチン開発企業の知的財産窃取（2020年） ・米国企業製ネットワーク管理ソフトウェアへの攻撃（2020年）
	Sandworm（APT44）	ロシア連邦軍参謀本部情報総局	・ウクライナ大規模停電（2015、2016年） ・米国大統領選挙有権者情報の窃取等（2016年） ・韓国・平昌冬季五輪大会の妨害（2017年）
	Cadet Blizzard		・ウクライナ政府機関等への侵入（2022年～）
北朝鮮	Lazarus（APT38）	朝鮮人民軍総参謀部偵察総局	・ソニーピクチャーズのシステム破壊・情報窃取（2014年） ・バングラデシュ銀行からの約8,100万ドル窃取（2016年） ・ランサムウェア「WannaCry」による攻撃（2017年） ・暗号資産取引所等からの暗号資産窃取（2017年～）
	Kimsuky		・米国等の組織・個人に対する標的型メール攻撃（～2024年）
	Andariel		・米国等の防衛・宇宙・原子力・エンジニアリング分野を狙った情報窃取（2024年）

（欧米政府当局等の発表に基づき当庁作成）

日本政府が公表している国家を背景としたサイバースパイ・サイバー攻撃の事例は、ほとんどが、日本が「仮想的」とみなす諸国に関するもので、いわゆる「同盟国」の事例は極めて稀だ。しかし、

- 同じ行為は米国なども実践しているはずであり、日本もスパイ・攻撃の主体になろうとしていることは間違いない。
- スパイや攻撃の「犯人」を証拠に基いて明かにすることは極めて困難。右図にあるように「疑われる」と述べるしかない。（アトリビューション問題）

公安調査庁「内外情勢の回顧と展望」2025
https://www.moj.go.jp/content/001437644.pdf

APTの事例からわかること

サイバースパイなくしてサイバー攻撃はありえない。攻撃に着目するだけではなく、スパイ活動に着目する必要がある。

- **身元の秘匿と長期潜伏**が可能な体制をとるだろう。
- 諸外国が実践していることは日本政府も実践する技術的能力があるはずだ、と考えるべき。実践の障害になっている法制度などを取り除き、**APTのような活動を行いたい、というのが日本政府の本音**だろう。
- 米国など「同盟国」と連携した作戦をとる場合、**「同盟国」の情報機関のカウンターパートナーとなる組織が必要**だという認識もあるだろう。
- 「能動的」とか「先制的」といった言葉を当て嵌めることが困難なために、**受動的とか自衛の枠組の歯止めがそもそも意味をなさない**。
- 今回は詳しくは述べられなかったが、スパイ・攻撃のためには、**民間企業の協力が必須**である。この点は別途テーマとしたい。

参考

高度持続的脅威（APT）とは

以下は一般的なサイバー攻撃についての手順として解説されているケース。APTの場合と大きな違いはない。

1. 偵察 初期の足場確保
2. 攻撃に必要な環境の準備
3. マルウェアを標的組織に配送
4. 標的組織の人をコントロール(ソーシャル・エンジニアリング)
5. システムの脆弱性への攻撃
6. 標的のシステムへの持続的なアクセス確保
7. 標的システムによる防御回避
8. 標的システム内の感染した端末を制御するコマンド&コントロールサーバとの通信確立

参考 株式会社ステラセキュリティ、小竹泰一「サイバー攻撃はどのように進行するか」『ポートスキャナ自作ではじめるペネトレーションテスト』、p.5 オライリージャパン。

上記のプロセスは、標的の組織へのスパイ活動(情報収集)の場合も、サイバー攻撃を行なう場合も、共通して実施される。

参考

高度持続的脅威（APT）とは

以下も一般的なサイバー攻撃のケースについての説明だが、APTにもあてはまる。

標的ネットワーク内での攻撃

1. 侵害した端末ではアクセスできないネットワークへの侵入⇒システムのユーザー情報、セキュリティ情報、他のシステムとの接続情報などを探索⇒より上位の権限の取得⇒パスワードなど認証情報の収集・窃取⇒取得した認証情報をもとに他の端末に侵入

2. 最終目標の達成

サイバースパイの場合

目的とするデータの収集(USBメモリ、Googleドライブなどクラウド、社内のチャット、メール、キーボード入力(キーロガー)、マイク・カメラのデータなど)⇒検知を回避して収集データの持ち出し

サイバー攻撃の場合

サービスの停止、コンテンツの改竄、データの削除、暗号通貨の窃取、データの暗号化(ランサクウェア)など

右文献を参考にした。 株式会社ステラセキュリティ、小竹泰一『ポートスキャナ自作ではじめるペネトレーションテスト』、オライリージャパン。

スパイ機関創設をめぐるこれまでの経緯

- 自民党総裁選挙の公約にスパイ機関創設を盛り込む

> **サイバーセキュリティ対策の強化**
> ・高度なサイバー攻撃やサイバープロパガンダ・偽情報に対応できる技術開発・人材育成を加速し、関連産業群を構築します。

> ・インテリジェンス関係省庁の司令塔としての「国家情報局」の設置、「スパイ防止法」の制定に着手します。https://storage2.jimin.jp/pdf/election/results/sousai25/findings/takaichi_sanae.pdf

- 10/20 自民・維新連立政権合意書 6項目の「インテリジェンス政策」が含まれる。
- 10/21 高市内閣第一回閣議「基本方針」

https://www.kantei.go.jp/jp/content/20251025hatsukakugi.pdf

「外交力、防衛力の強化」の項目で「インテリジェンス機能の強化に取り組む」

- 10/24 木原官房長官記者会見(午前)記者の質問に「国家情報局」の創設に向けて検討を進める意向を表明。「戦後最も複雑で厳しい安全保障環境のなかでわが国の国益を守り国民の安全を確保するためにはインテリジェンスにおける国家機能の強化が急務」
- 11/4、6に維新、参政が国家情報局設置に賛成の発言
- 11/14 自民党、インテリジェンス戦略本部初会合。政府のインテリジェンス（情報収集・分析）活動の司令塔組織となる「国家情報局」創設に向けた議論を開始

スパイ機関創設をめぐるこれまでの経緯
自民・維新の合意文書に書かれていること

10/20 自民、維新連立政権合意書 6項目の「インテリジェンス政策」が含まれる。

https://o-ishin.jp/news/2025/images/624de5f22900f6e88e892abb49d3fc70ef3cac92.pdf

- 内閣情報調査室と内閣情報官を格上⇒「**国家情報局**」及び「国家情報局長」を創設
- 「国家情報局」及び「国家情報局長」は、「国家安全保障局」及び「国家安全保障局長」と同格
- 現在の「内閣情報会議」(閣議決定事項)を発展的に解消⇒2026年通常国家において、「**国家情報会議**」を設置する法律を制定
- 2027年度末までに独立した**対外情報庁(仮称)**を創設
- 2027年度末までに、**情報要員(インテリジェンス・オフィサー)養成機関**を創設
- インテリジェンス・スパイ防止関連法制(基本法、外国代理人登録法及びロビー活動公開法等)について令和7年に検討を開始し、速やかに法案を策定し成立

合意文書で述べられていることの大半は、スパイ機関の創設に関するものであり「スパイ防止」には力点が置かれていない。にも拘わらず「スパイ防止法」と呼んだのは政権の偽旗作戦だ、と思う。

スパイ機関創設をめぐるこれまでの経緯
自民・維新の合意文書に書かれていること

外国代理人登録法について

小林氏、外国勢力の登録義務化を　スパイ防止法念頭
「自民党小林鷹之政調会長は30日の記者会見で、スパイ防止法の制定を念頭に、**外国勢力やその代理人が日本国内で情報収集活動する場合に登録を義務付ける制度**が必要との考えを示した。米英両国の外国代理人登録法に触れ「外国勢力の情報収集活動を国民の監視下に置くルールがあってしかるべきだ」と述べた。」(共同)https://www.47news.jp/13383975.html)

ロビー活動公開法について
ロビー活動開示法ともいう。登録法とセットで運用される(と思う)。

参考 JETRO 「国における政策策定プロセスとロビー活動にかかる調査報告書」
https://www.jetro.go.jp/ext_images/_Reports/02/2017/7f0f9e9b7bed9b62/report1703_1.pdf

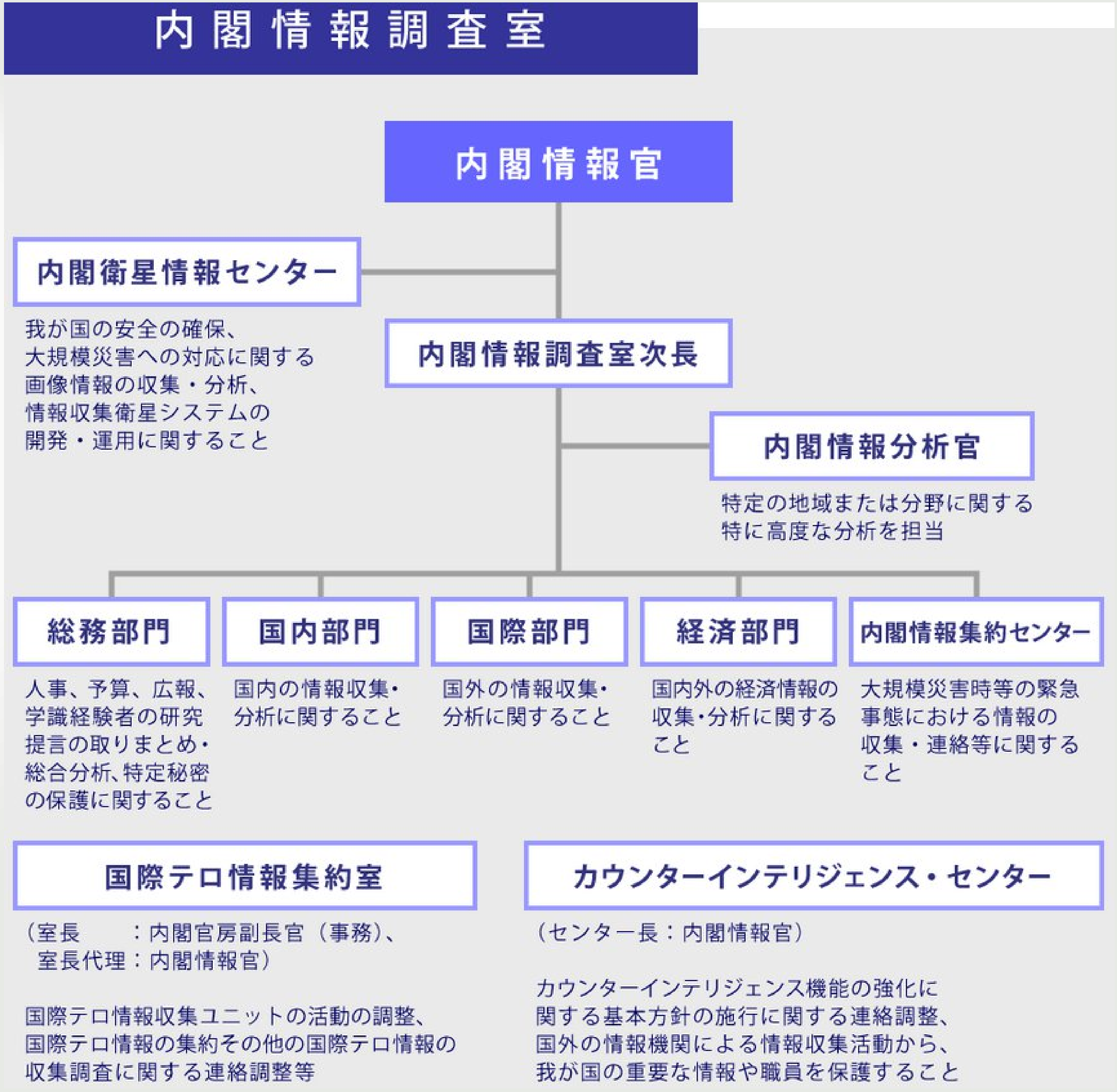
海外の団体と連携して活動している日本国内の団体、あるいは外国に出自をもつ日本国内の団体への監視や規制の仕組みになりかねない。

参考

内閣情報調査室

メディア（新聞、雑誌、専門誌、　通信社ニュース、テレビ、インターネット等）からの膨大な公開情報のほか、学識経験者や民間の専門家等の様々な情報源との意見交換によってもたらされる情報、情報収集衛星による画像情報を収集・整理し、国内外の諸情勢に関する分析業務を行っています。また、**外交・防衛・治安等の情報を担当する省庁によって構成されている「情報コミュニティ」の取りまとめ機関**として、これらの省庁が収集・分析した情報を集約し、内閣の立場から分析・評価を行っています。

https://www.cas.go.jp/jp/gaiyou/jimu/jyouhoutyousa/yakuwari.html



参考

内閣情報調査室 2025年度予算案

17. 内閣情報調査室 3,776(3,530)

安全保障と経済を横断する領域における課題の顕在化、中国による尖閣諸島周辺における領海侵入や領空侵犯、軍事活動の活発化、北朝鮮による核・ミサイル開発、国境を越えたサイバー攻撃や情報戦、東南アジアや欧米等に拡散する国際テロ等、我が国の安全保障上の脅威は極めて厳しい状況にある。また、国家安全保障の対象は、経済、技術等にまで拡大しており、有事・平時、軍事・非軍事の境目は曖昧になっている。こうした中、我が国の国益を確保し、国民の安全を確保するために適切な政策判断を下していくためには、情報部門がより多くの質の高い情報を効率的に収集、集約、分析した上で政策部門に提供し、その結果に基づいて政策決定が行われることが必要であることから、特に、情報収集機能強化に必要な基盤整備等を実施する。

○情報の収集及び分析その他の調査 2,520(2,293)

我が国の安全保障上の脅威やＩＳＩＬ等による「テロの脅威」等から、我が国の権益を保護し、国民の安全を確保することに資する情報の収集及び分析その他の調査に必要な基盤整備等を実施する。

○情報の収集調査委託 758(758)

多角的な情報の収集・分析及び有効かつ効率的な情報収集に資するため、情報の収集調査業務の一部を部外の団体に業務委託する。

○情報機能強化検討 214(222)

政府の情報機能の強化を図るため、サイバー空間における情報の収集及び分析その他の調査に必要な基盤整備等を実施する。

○カウンターインテリジェンス推進 284(257)

政府のカウンターインテリジェンス機能の強化を図るため、政府内における情報通信のセキュリティの強化に必要な基盤整備等を実施する。

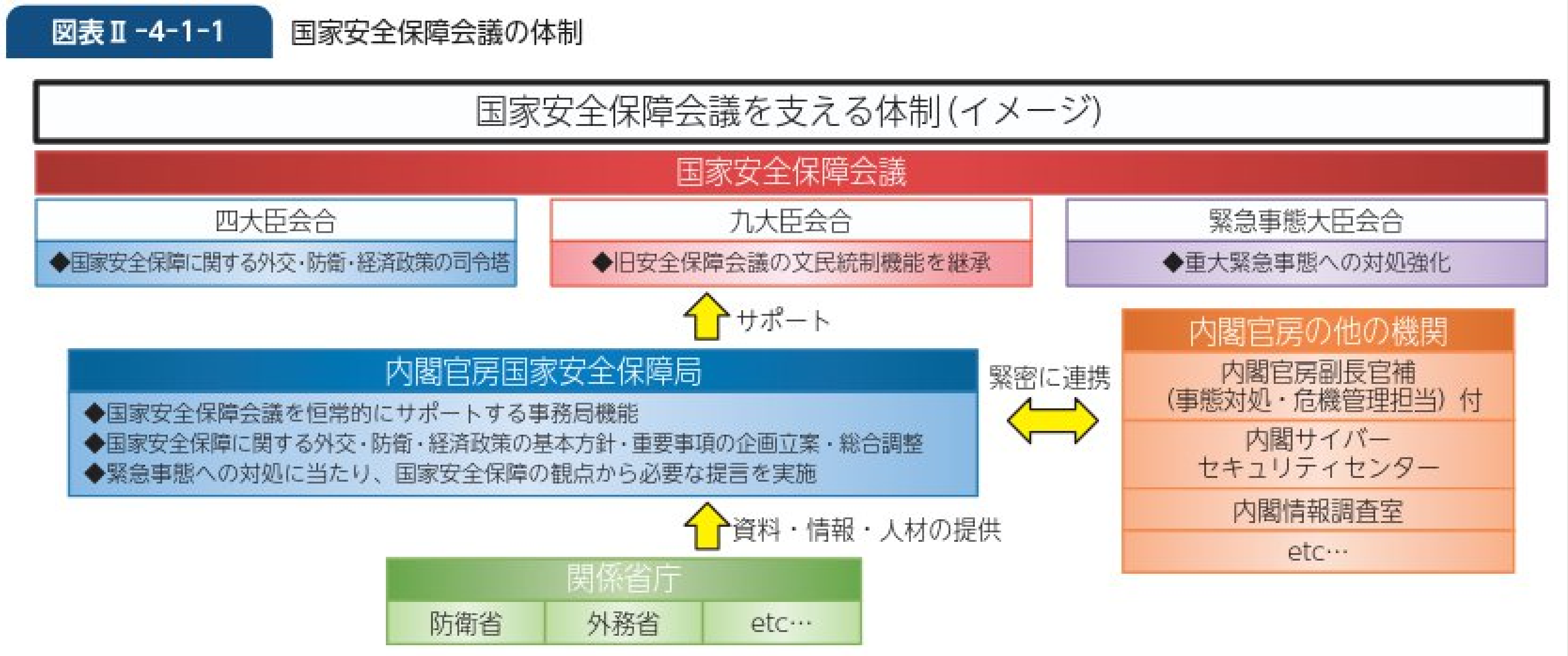
https://www.cas.go.jp/jp/yosan/pdf/r7_yosan_an.pdf

予算 37.8億円(カッコ内は昨年予算額)
このほかに関連する内閣衛星情報センターは、622.5億円と内閣官房のなかでも突出して巨額。
この分野は予算規模だけでその役割の大きさを評価してはならない。

参考

国家安全保障局と国家安全保障会議

国家安全保障局
業務
• 国家安全保障会議をサポート。内閣官房の総合調整権限を用い、国家安全保障に関する外交・防衛・経済政策の**基本方針・重要事項に関する企画立案・総合調整**に専従。
• **緊急事態への対処**に当たり、国家安全保障に関する外交・防衛・経済政策の観点から必要な提言を実施。(事態対処のオペレーションは、危機管理の専門家である内閣危機管理監等が引き続き担当。)
• 関係行政機関等に対し、適時に情報を発注。また、会議に提供された情報を、政策立案等のために活用(情報の「総合整理」機能)。



https://www.cas.go.jp/jp/gaiyou/jimu/anzenhosyou.html

参考

国家安全保障局と国家安全保障会議

国家安全保障会議設置法第二条　会議は、次の事項について審議し、必要に応じ、内閣総理大臣に対し、意見を述べる。
一　国防の基本方針
二　防衛計画の大綱
三　前号の計画に関連する産業等の調整計画の大綱
四　武力攻撃事態等（武力攻撃事態及び武力攻撃予測事態をいう。以下この条において同じ。）又は存立危機事態への対処に関する基本的な方針
五　武力攻撃事態等又は存立危機事態への対処に関する重要事項
六　重要影響事態への対処に関する重要事項
七　国際平和共同対処事態への対処に関する重要事項
八　国際連合平和維持活動等に対する協力に関する法律（平成四年法律第七十九号）第二条第一項に規定する国際平和協力業務の実施等に関する重要事項
九　自衛隊法（昭和二十九年法律第百六十五号）第六章に規定する自衛隊の行動に関する重要事項（第四号から前号までに掲げるものを除く。）
十　国防に関する重要事項（前各号に掲げるものを除く。）
十一　国家安全保障に関する外交政策、防衛政策及び経済政策の基本方針並びにこれらの政策に関する重要事項（前各号に掲げるものを除く。）
十二　重大緊急事態（武力攻撃事態等、存立危機事態、重要影響事態、国際平和共同対処事態及び次項の規定により第九号又は第十号に掲げる重要事項としてその対処措置につき諮るべき事態以外の緊急事態であつて、我が国の安全に重大な影響を及ぼすおそれがあるもののうち、通常の緊急事態対処体制によつては適切に対処することが困難な事態をいう。第三項において同じ。）への対処に関する重要事項
十三　その他国家安全保障に関する重要事項

国家安全保障会議は安保・防衛3文書は国家安全保障会議で検討し、後に閣議決定された。3文書改訂も同様の手順を踏む

サイバースパイ・サイバー攻撃全体像

サイバースパイ・サイバー攻撃には様々な手法があり、手法ごとに、その効果も異なる。目的も以下のように様々である。(次ページ以降の表参照)

- 侵入のための情報収集
- 機密情報の収集
- 不正サイトへの誘導
- ネットワークへの不正接続
- ネットワークを支える中心のコンピュータ(ホスト)への侵入
- 管理者権限の奪取
- セッションの乗っ取り(通信の開始から終了までの間のデータのやりとりを横取りする)

スパイと攻撃両方にあてはまる目的

- 不正な処理・機能の実行
- システムやデータの破壊・改竄
- サービス妨害
- 金銭

システムを破壊するなど明確な攻撃目的

出典 上原孝之 『情報処理教科書・情報処理安全確保支援士』2025年版

	侵入のための情報収集	機密情報の収集	不正サイトへの誘導	ネットワークへの不正接続	ホストへの侵入	管理者権限の奪取	セッションの乗っ取り	不正な処理・機能の実行	システムやデータの破壊・改竄	サービス妨害	金銭
アドレススキャン(pingスイープ)	○										
ポースキャン	○										
スタックフィンガープリンティング	○										
パケット盗聴	○	○									
DNSサーバからの情報収集(不正なゾーン転送要求)	○										
ソーシャルエンジニアリング	○	○									
フィッシング(Phishing)		○	○								
DNSキャッシュポイズニング		○	○				○				
ウォードライビング(無線LANへの不正接続)				○							
パスワードクラック				○	○	○					
セッションハイジャック		○		○			○				

	侵入のための情報収集	機密情報の収集	不正サイトへの誘導	ネットワークへの不正接続	ホストへの侵入	管理者権限の奪取	セッションの乗っ取り	不正な処理・機能の実行	システムやデータの破壊・改竄	サービス妨害	金銭
ARPポイズニング				○			○				
セッションフィクセーション		○		○	○		○				
バッファオーバーフロー		○			○	○		○	○	○	
クロスサイトスクリプティング(XSS)		○	○				○	○	○		
SQLインジェクション		○	○					○	○	○	
OSコマンドインジェクション		○			○	○		○	○	○	
HTTPヘッダインジェクション		○	○				○	○	○		
メールヘッダインジェクション			○					○			
ディレクトリトラバーサル攻撃		○				○					
サーバーサイドリクエストフォージェリ(SSRF)			○		○			○	○	○	
クロスサイトリクエストフォージェリ(CSRF)							○	○		○	

	侵入のための情報収集	機密情報の収集	不正サイトへの誘導	ネットワークへの不正接続	ホストへの侵入	管理者権限の奪取	セッションの乗っ取り	不正な処理・機能の実行	システムやデータの破壊・改竄	サービス妨害	金銭
DoS攻撃									○	○	○
スパムメール			○								
マルウェア(ウィルス、ワーム、ランサムウェア、ボットなど)	○	○	○	○	○	○	○	○	○	○	○
クリックジャッキング攻撃			○					○			
標的型攻撃		○	○					○			○
ビジネスメール詐欺(BEC)											○
SEOポイズニング			○					○			

出典 上原孝之『情報処理教科書・情報処理安全確保支援士』2025年版p.98

サイバースパイ・サイバー攻撃全体像

- **官民連携なしに、スパイも攻撃もできない。**

  自衛隊や警察など政府機関だけでは遂行できない。**民間がスパイ・攻撃の主体**になる可能性がある。
  自国の民間企業との連携だけでは限界がある(米国の**ビッグテックの協力**が不可欠)。
  攻撃の手段によっては、一般の人たちが保有する**スマホ、パソコンを武器化**可能である。
- **標的のシステムのセキュリティを突破することも「攻撃」**である。サイバースパイはサイバー攻撃と不可分。能動的と受動的、先制と自衛は表裏一体で境界を引くことはできない。
- **長期にわたり標的のシステムに潜伏**する技術が必須。
- **身元を秘匿する**(攻撃者としての名乗りを上げない)ことが多い。日本もスパイ・攻撃で自ら名乗りを上げるとは考えにくい。(チェック機能が働かない)
- **サイバー領域で完結しない。**

私たちの対抗手段について

日本国内にいる私たちが標的になる？

- 日本政府が国家の重要な経済インフラとみなす施設などへの抗議行動を経済安保を口実に監視の標的にすることがありうる。(原発、巨大開発事業から国策としての大規模イベントへの反対運動など)
- 市民運動、労働運動に関して従来から行なわれてきた監視や治安弾圧がサイバー領域において、政府のスパイ活動とともに、これまで以上に巧妙に拡大される。
- 日本政府が国内外の反政府運動や、日本政府が「敵」とみなす国の出身者を監視するなどの目的で、従来の法制度では困難だったスパイ行為を実行する可能性がある。
- 「同盟国」の安全保障のために、「同盟国」と連携した監視などを行う可能性がある。(たとえば、基地反対運動など)
- 日本を「敵」とみなす国などの組織から標的になりうる。

私たちの対抗手段について

サイバースパイ・サイバー攻撃の「入口」としてよく用いられるのは

- メールなどの添付書類にマルウェアなどを仕込む
- ルーターなどのネットワーク機器の脆弱性を利用する
- パスワードを窃取されてなりすまされる

- システムやソフトウェアを常に最新の状態に保つ
- Wi-Fiなどの機器についてもセキュリティ対策をとる
- パスワードの基本を守る(使い回しはしない、推測されやすいものは使わない、長い文字列を使う)

私たちの対抗手段について

通信事業者や企業や学校などのネットワーク管理会社、SNSのプラットフォーマーなどが、政府との協定に基づいて、私たちの通信を監視し、データを政府などに提供する場合への対処

- 政府と協定を結んでいない信頼できる通信事業者のサービスを選ぶ。
- サービス提供事業者もユーザーのデータや動向を把握できない「ゼロナレッジ」のサービスを選ぶ。
- パスワード管理をルール通りにする。

などできることは多くあります。大切なことは

- 自分のコミュニケーションの権利を政府や警察に委ねない。
- コミュニケーションやプライバシーの権利を利益のために犠牲にする企業のサービスは可能な限り使わない。

私たちの対抗手段について

しかし...

- 自分のコミュニケーションの権利を**政府や警察に委ねているの**かどうかをどう判断できるの？
- コミュニケーションやプライバシーの権利を**利益のために犠牲する企業のサービス**かどうかをどう判断する？

たぶん、これまで通りの「あたりまえ」と思ってきたネットの使い方だけでは気づけないことも多いはず。**気づくこと、ライフスタイルを変えること、これが一番の難問**かもしれません。

JCA-NETのセミナーはこうした「難問」に皆で取り組む場にできればと考えています。よろしくお願いします。